EXHIBIT T

Privacy & App Review

Key Concepts

- Smart Phones represent the new frontier in advertising
- Smart Phones, unlike computers, cannot easily be cleared of tracking methods
    - Such as Cookies on a computer
- Developers have a relationship with Marketers because they're the revenue source for free Apps

Apps and Privacy Statistics

- 33% of free iPhone Apps have the capability to access a user's location
    - Compared to 29% on Android
- 14% of free iPhone Apps have the capability to access a user's contacts
    - Compared to 8% on Android
- 23% of free iPhone Apps include third-party code (code not written by the developer)
    - Examples: code that enables mobile ads to be served or analytic tracking for developers
    - Compared to 47% of Android

Difficult Relationship #1: Marketers and Developers

Developers want to reach customers. However, in the World of Apps, perhaps no factor is more important to potential customers than the price. A user is infinitely more likely to try out an App that is free because they believe they won't lose any money, and if they don't like the App and can delete it.

However, Developers need to make money to support themselves and their App production. If they cannot get customers to pay, they turn to the other strong source of revenue: advertising. This mobile advertising concept includes market research companies, advertising agencies, marketing strategists, and more. Marketers provide Developers with code to input into their Apps to both gather information about the user, as well as display some form of advertisement. Even if a Developer feels it is unethical to harvest their users' information, they feel as if they have little choice due to their financial situation. Marketers provide a solution: bring us users and we'll pay you...bring us even more uses, and will pay you more. "Some developers feel pressure to release more data about people. Max Binshtok, creator of the DailyHoroscope Android App, says ad-network executives encouraged him to transmit users' locations." (WSJ)

Marketers provide Developers with code to embed in their Apps, and often times this code does more than the Developer thinks it does: "We found that not only users, but developers as well, don't know what's hAppening in their own Apps, which is fascinating" (Safeinternet.org). To get the most out of their

investment, marketers want to collect as much data as possible, which sometimes means collecting more data than even the Developers realize.

What Are Marketers After?

Users are *unknowingly complacent* in this process. People are willing to tolerate advertising in Apps if they can get the App for free. However, rarely does the consumer know that their new App is transmitting information about them, and even fewer know to whom it is transmitted to. There are many important pieces of demographic information that can be accessed by Apps on the iPhone, and marketers want them all:

- **Usernames and Passwords**
    - Being able to know a person's username across multiple places (such as social networking sites or personal finance Apps) allows marketers to know everything about an individual's online life
        - This helps marketers place advertisements custom tailored for specific users across all of the any and all platforms where this user might see them
- **Contacts**
    - Accessing a phone's contact list provides a marketing firm with the personal information of everyone that a user knows, further helping build databases rich in demographic information.
- **Age/Gender**
    - Marketers want to know a user's age and gender for demographics research.
    - Knowing what habits people of certain ages and genders have on their smart phones (ex. what Apps they use, where they're located, etc.) can help marketers create advertising that targets specific ages and genders.
- **Location**
    - Many see location-based advertising as a potentially huge opportunity. By accessing a user's current location, marketers can pump in ads that pertain to a user's immediate surroundings.
- **UDID**
    - Every device has a unique identification number (UDID). If a marketer can track a UDID across numerous Apps, they can begin to collect information on the user's patterns and habits from multiple sources.
    - The UDID has been called the "supercookie" (as a comparison to cookies on computers) to explain its significance for being able to track a user
        - "The great thing about mobile is you can't clear a UDID like you can a cookie...that's how we track everything" (WSJ)
    - The UDID is controversial because marketers claim that it is Non-Personally Identifiable Information because it isn't tied to a user's name. However, many consumer-advocacy groups believe it to be just as personal as a user's name, address, or other information directly tied to the user.
- **Phone Number**
    - Area code can be used for demographic information harvesting

Josh Hornthal, Apple Inc. 2011

Who Are These Marketers?

According to the Wall Street Journal, Google was the biggest recipient of the data transmitted in these tests.

- Specifically AdMob, AdSense, Google Analytics and DoubleClick
    - 38 of the 101 Apps tested by the WSJ sent data to Google

So What's Apple Doing?

Apple has policies that require a user to give consent whenever their personal data is accessed. Even if Apple believes the Apps that pass its review process, the reality is this policy is not followed by Developers:

- Among the Apps tested by the WSJ, iPhone Apps transmitted more data than Apps on Android
- Of the 101 smartphone Apps WSJ examined, 56 transmitted the phone's UDID to other companies without users' awareness or consent.
- Forty-seven Apps transmitted the phone's location without consent
- Five sent age, gender and other personal details to outsiders without consent

Smart Phones, including the iPhone, don't do a good job of informing users of all of the types of information that Apps harvest from their phones. Apple needs to be the industry leader and take a major step towards informing users about what's actually going on with their Apps. Apple does a good job of informing users when an App wants to access their current location, however it's clear that Apps are harvesting more information than just current location, and users should have the power to decide who can access what.

Difficult Relationship #2: Apple and Apple

Apple has put itself into a difficult position: finding a balance between iAd's needs for demographic data that every advertising firm needs to thrive and Apple's stance on privacy. Apple has incredible access to user information through Apple IDs, but with great power comes great responsibility. If Apple can take a stand against uninformed users, they stand to benefit from both the PR, as well as an increase in iAd revenue that will come from iAd customers wanting to align with Apple's favorable public image.

Josh Hornthal, Apple Inc. 2011